In response to Proceeding 07-52:

With regard to:
8. "We seek a fuller understanding of the behavior of broadband market participants today..."

Packet management today is used primarily as a security measure or a means to provide quality of service on a congested network to content which is generally accepted as being more important. Two examples of this are mitigating SPAM, limiting use of peer-to-peer traffic, and filtering and/or reacting to any type of attack (DDoS, botnets, malicious activity). However, these are the simple cases where packet based management may or may not affect user traffic.

While IP packets do have information which can be used to identify destination and traffic type, there is further classification of traffic other than the general details of a packet, which, in some circumstances, is encapsulated, which makes determining discrimination baseless. For example, the HyperText Transfer Protocol (HTTP) is used to request and send content to and from a user and/or server. Typically it is used in a manner where a user requests a web page via a web browser and a web server sends the content back to the user's browser via HTTP. However, HTTP is also used in other "applications"; one such application is BitTorrent. In the case of BitTorrent, HTTP is used by the user of a peer-to-peer client application to request a list of more 'peers' for which content is then downloaded from the peers rather than an individual server. While it can be used for any purpose, the traffic generated by BitTorrent traffic can become very aggressive - creating thousands of connections and in many cases generates too much congestion for an ISP to maintain quality of service to other users. As such, many ISPs limit the BitTorrent application by either intercepting requests to the peer 'server' or simply by limiting the traffic between peers. Would this be discrimination? If this case is considered discrimination then this limits an ISP's ability to manage traffic to maintain reliability for all users. If this example is not considered discrimination then it specifically allows discriminating other forms of traffic simply by claiming that one packet affects congestion more than another. The conflict is not in whether a packet discriminates or not, it's that there is currently not facilities or equipment to determine which packets are causing the congestion. Today's equipment is built to route traffic based on the IP headers of the packet. Because the IP protocol itself does not define routing or priority based on the payload (data), a great amount of processing is required to inspect the contents of a packet and determine what is causing congestion. In order to do so, not only would the equipment have to inspect the data, it would also have to "remember" what IP source and destinations are generating what traffic; only then could the equipment determine not only what type of traffic, but what IP nodes are causing the congestion; then the equipment could make a decision which entails managing packets which affect the service of users. The idea of "innocent until proven guilty" applies here - the equipment doesn't know which traffic to manage or what traffic is causing congestion until it has all the evidence; not only does

equipment have to perform this processing, you must take into account that if the network is congested in the first place, the equipment maybe too busy to figure out the problem and more importantly may not take into account all of the evidence for the fact that packets can be dropped somewhere else in the network and may never be seen by the equipment. In order to cope with this, ISPs which determine a particular application is causing congestion on their network will transparently reduce the ability of the application's packets to congest the network. In the case this actually affects the quality of service for a user, the user can call the ISP and request he be "white-listed" in the blanket packet management system so his quality is not affected. This is typical practice by many small ISPs but often times large ISPs will not care and in fact may have terms of service limitations specifically limiting the user from emitting congestion-causing traffic in the first place. In short, the definition of 'discrimination' with regard to packet management is a case-by-case scenario and regardless of new rules, it will be near-difficult to enforce because neither the FCC, the consumer, nor the service provider control the affect of a packet's activity with regard to the quality of other services.

http://www.dslreports.com/shownews/56419

9. "9. Next, we ask commenters to describe today’s pricing practices for broadband and related services."

Typically broadband service providers do not sell or practice selling different services based on content or delivery. Service providers sell based on availability,reliability commitments, and speed. For example, some providers may state that any circuit downtime will result in a credit to the user's bill, where as others may specifically state that outages should be accepted regardless of the service sold. Obviously there are consumer protection rules (telecommunications act) which cover any exploitation with regard to service interruptions. Typically if a service provider advertises better service for particular content, such as games, the provider has built a better IP infrastructure in general and the improved service applies to all content, not just what is marketed. For example, building a low-latency network will make online video games faster REGARDLESS of whether a user has 1.5mbps of bandwidth or 35mbps of bandwidth. However, latency is less important in applications like e-mail but more bandwidth will enable faster download times. A service provider which builds a low latency network may advertise to consumers of content which would benefit from the network, regardless of whether packet management is used or not.

Pricing of bandwidth is only falling in areas where multiple broadband options are available. Pricing of bandwidth has gone up in areas where there is only one provider. ILEC bandwidth pricing, with the exception of Verizon FIOS, has not gone down. Pricing of bandwidth from cable providers has not gone down and service limitations, such as the amount of traffic transferred, is often exercised.

If you add more regulations, the regulated will just increase prices (and do less):

http://news.com.com/2100-1034-5185215.html

10. "10. We next ask whether the Policy Statement should be amended."
It would be in the best interest of consumers for the entire policy to be less focused on discriminating traffic and more focused on informing a consumer on any packet management, not allowing discrimination based on destination (whether local or not) and allowing for complaints of unfair practices. Currently, there are too many loop holes which still allow discrimination simply by encapsulating the content or not allowing the content to traverse the Internet. By simply stating that discrimination is based on source and destination, ISPs are free to remain neutral, and yet are still limited from practices which will limit a consumers ability to freely connect to services.

Regardless of whether commission may or may not have jurisdiction to enact and/or enforce the Policy Statement, the Internet, IP traffic, and the networks and content they provide are naturally neutral. Trying to classify what actions on the network are or are not discrimination will be an endless process simply because the Internet never stops changing or growing and as such is dynamic enough that you will never be able to both classify it and regulate it both at the same time.

IP content is different to different destinations and neither the content or the destination are aware of each other - just as nobody can realistically be aware of the many ways an individual perceives the colour Red - nobody can realistically be aware of the many ways packets on the Intenret, it's protocols, or it's network may or may not be used.

It's a waste of tax-payer money to continue enacting any rules with regard to Internet content. They are implicitly rhetorical because, regardless of whether the start or end points are the user or ISP, physical connections, throughput, and IP headers are the only open components of Internet connectivity. All of the content, which may or may not be open, is generated by a user.

It is also impossible to classify any type of traffic as local to an ISP if it's on the Internet, or the user has an Internet connection, because the user can always route the traffic back onto the Internet and thusly the ISP would then be discriminating against traffic which is then leaving the local ISP network.